

Problem set 5

December 29, 2015

Due: January 12

- Please submit the handout in class, or email the grader (omer.rotem1 at gmail.com).
- Write clearly and shortly using sub-claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution” w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- It is allowed to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write his solution by *himself* (joint effort is only allowed in the “thinking phase”)

- (a) Let (E, D) be a perfectly correct encryption scheme for messages of length n and keys of length ℓ . Let $K \leftarrow \{0, 1\}^\ell$. For each of the following cases find the best lower bound for ℓ .
- i. $D(E_K(m_0)) \parallel E_K(m_1) \leq \varepsilon$ for any $m_0, m_1 \in \{0, 1\}^n$.
 - ii. $\text{SD}(E_K(m_0), E_K(m_1)) \leq \varepsilon$ for any $m_0, m_1 \in \{0, 1\}^n$.
- (b) Let $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ be (s, ε) -OWF, and let $\mathcal{H} = \{h: \{0, 1\}^n \mapsto \{0, 1\}^n\}$ be 2-universal family. Define g over $\{0, 1\}^n \times \{0, 1\}^n \times \mathcal{H} \times [n]$ by $g(x, r, h, i) = (f(x), r, h, h(x)_{1,\dots,i}, b(x, r))$, for b being the Goldreich-Levin hardcore predicate (i.e., $b(x, r) = \langle x, r \rangle_2$). Find good as you can vales for s' and ε' such that $g(U_{2n}, H, I)$ has (s', ε') -entropy $H(g(U_{2n}, H, I)) + \frac{1}{2n}$, for $H \leftarrow \mathcal{H}$ and $I \leftarrow [n]$. You can assume that \mathcal{H} can be sampled and evaluated by a size n circuit.